UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/499,720	02/08/2000	Dale C. Morris	10991915-1	1658

22879   7590   10/29/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
ROJAS, MIDYS

ART UNIT	PAPER NUMBER
2185	

MAIL DATE	DELIVERY MODE
10/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	09/499,720	MORRIS ET AL.
	Examiner	Art Unit	
	Midys Rojas	2185	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _07 August 2007_.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-24_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-24_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _02 August 2000_ is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments, filed on 8/07/2007, with respect to original claims 1-24, have been fully considered but they are not persuasive.

Applicant argues that instruction memory 36 of the Arora Patent is a cache memory for storing instructions that are processed in the pipeline 32, thus instruction memory 36 does not include a first page of memory not writeable by application instructions at a first privilege level. Instruction memory 36 is a cache memory where all instructions are stored for execution. The Arora Patent discloses that a typical pipeline 32 includes a stage during which instructions are fetched from the memory 36. (Col. 3, lines 44-46).

Furthermore, Applicant argues that the Banning Patent also fails to teach or suggest a privilege promotion instruction being stored in a first page of memory not writeable by application instructions at a first privilege level and that there is no teaching or suggestion for one skilled in the art to combine the cache memory of the Arora Patent with the T bit system of the Banning Patent. Cache memories store data temporarily, therefore one skilled in the art would not implement the T bit system of the Banning Patent to protect instructions temporarily stored in the cache memory of the Arora Patent from being overwritten. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed.

Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the

Arora patent already teaches storing a privilege promotion instruction in a memory. The Arora

patent does not teach the instruction memory including a page of memory not writeable by

application instructions at a first privilege level. Banning et al. discloses an instruction memory

where memory pages marked with at T bit are protected and if a write is attempted, an exception

is generated (Col. 1, line 60 – Col. 2, line 8). In this system, the T bit provides the protection so

that the memory page is not writeable at the first privilege level. It would have been obvious to

one of ordinary skill in the art at the time the invention was made to replace the instruction

memory of Arora with an instruction memory employing instruction memory protection, as

disclosed by Banning, since doing so provides for valid, un-tampered memory instructions by

protecting these instructions from being overwritten or changed. Even though Arora teaches an

instruction memory in the form of a cache, thus being temporary and not needing protection, this

instruction memory is being replaced by the instruction memory of Banning, which suggest the

need for instruction protection to prevent the overwriting of already translated instruction and/or

to prevent the use of invalid translations (see Col. 1, line 53 – Col. 2, line 35).

For applicant's other arguments, the examiner would like to point out that Applicant

bases most of his arguments on the labels being given by the Arora patent to the various

privilege levels it employs. The Examiner would like to explain that regardless of what the

privilege levels are labeled as by the Arora Patent, the examiner is free to interpret the true

meaning and relationship of these privilege levels within the system of Arora.

Applicant argues that the Arora patent does not teach reading a stored previous privilege

level state and comparing the read previous privilege level state to the current privilege level

since in the Arora patent a previous privilege level state is not stored and therefore cannot be read. However, the Examiner maintains that the previous privilege level state is stored in CPL 38 since a **prior** instruction would have set the CPL 38 to the proper privilege level and the CPL is maintained (stored) in the processor's register set. Then the CPL is compared to the privilege level of the EPC in the process of determining if the fetched instruction requires the processor to change the privilege level from a first level to a second level (Col. 5, lines 40-50).

Applicant argues that the privilege level of the EPC instruction does not teach or suggest the current privilege level. Rather, the EPC instruction directs the processor to change the privilege level of the CPL and provides a future privilege level, not the current privilege level. Applicant notes that the CPL is the current privilege level, not the previous privilege level state, and the privilege level of the EPC instruction is a future privilege level, not the current privilege level as submitted by the examiner. However, as interpreted by the examiner and regardless of the labels being given to the respective privilege levels of the invention, at the moment of comparison, the privilege level of EPC is the privilege level necessary for the instruction that is **currently** being prepared for execution in the system (instruction requiring a higher priority level follows in the pipeline), thus it is a **current** privilege level. Also, at the moment of comparison, the CPL is the previous privilege level because it was the privilege level set by a prior instruction (Col. 4, lines 19-28), and it is the privilege level that was necessary for the execution of an instruction that was executed previous to the instruction corresponding to the EPC. Therefore, for interpretation purposes, at the moment of privilege level comparison, the EPC represents the current privilege level and the CPL represents the previous privilege level.

With this in mind, Arora does teach comparing the read previous privilege level state to the current privilege level.

Applicant mentions that the CPL remains the current privilege level during the execution of the EPC instruction and it is therefore, the current privilege level and not the previous privilege level. However, the privilege level was set by a previous instruction and so, it is considered to be a previous privilege level. Once the CPL is updated when the EPC is executed, the CPL will take on the value of the EPC and will become the new previous privilege level since it was set by the previous instruction. The new EPC will become the new current privilege level.

Applicant argues that the Arora patent does not teach comparing a read previous privilege level state to the current privilege level state. However, Arora teaches comparing the CPL to the EPC wherein the CPL is stored in the CPL register 38 and must be read from there in order to perform the comparison.

Applicant argues that the Arora patent does not disclose promoting the current privilege level to a second privilege level, which is higher that the first privilege level if the previous privilege level state is equal to or less privileged that the current privilege level. However, as maintained by the examiner, when the CPL and the EPC are compared, if the previous privilege level, which is stored in the CPL, is set to a lower privilege level (less privileged) than the current privilege level, indicated by the EPC (CPL is set to level 3 and EPC is set to level 0, Col. 6, lines 46-61) then, the current privilege level is promoted (in this example, to level 0) as the processor operates at the higher privilege level of the EPC. After the EPC instruction is retired, the CPL will take on the privilege level previously represented by the EPC and therefore, this

will become the new previous privilege level. For the purposes of the examiner's rejection, the

CPL represents the previous privilege level and the EPC represents the current privilege level;

the promotion or increasing of the privilege level is represented by the raising of the privilege

level to that of the EPC.

Applicant argues that the Arora patent does not teach a call instruction including storing

the first privilege level in a previous privilege level state. However, as stated in the applicant's

argument, the CPL (previous privilege level, as stated by the rejection) is stored when it is

increased at the time the EPC instruction is retired (page 13 of arguments). This process must

occur at the call of an instruction since the operation of the system is governed by the ·

instructions of instruction memory 36.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over by Arora

(6,393,556) in view of Banning et al. (6,363,336).

Regarding Claims 1 and 6, Arora discloses a method of promoting a current privilege

level ("change current privilege level to a higher privilege level" Column 6, lines 46-61) of a

processor of a computer system controlled by an operating system (Col. 1, lines 10-41) wherein

the current privilege level controls application instruction execution in the system by controlling

accessibility to the system resources (Column 1, lines 30-41), the method comprising:

performing a privilege level promotion instruction by the operating system (Column 4, lines 13-27, and Column 6, lines 46-61), the privilege promotion instruction being stored in a memory (instruction memory 36 storing a plurality of instructions... see Figure 2) wherein processing these instructions direct the processor to change the privilege level (privilege promotion instructions, see Col. 2, lines 19- 37), the privilege promotion instruction including:

reading a stored previous privilege level state (register CPL 38 stores the privilege level set by a previous instruction, Col. 4, lines 19-22),

comparing the read previous privilege level state (CPL 38) to the current privilege level (comparing CPL to the instruction's privilege level, indicated by the EPC, wherein this case the instruction's privilege level is the current privilege level and the stored privilege level is the previous privilege level, column 6, lines 46-49. The privilege level stored in CPL 38 is the previous privilege level since it represents a previous instruction, while the privilege level related to the EPC is the current privilege level since it represents the current instruction);

and if the previous privilege level state is equal to or less privileged than the current privilege level ("since the EPC instruction directs the processor to change the architectural privilege level to a higher privilege level..." indicates that the CPL is less privileged than the level indicated by the EPC), promoting the current privilege level to a second privilege level which is higher than the first privilege level ("...increase the architectural privilege level from privilege level 3 to privilege level 0" wherein privilege level 0 is more privileged). The privilege level is promoted as the processor starts to operate at the higher privilege level indicated by the EPC. In comparing privilege levels, the stored privilege level (stored in CPL 38) must be read in the comparison process.

Arora does not teach the instruction memory 36 including a page of memory not writeable by application instructions at a first privilege level.

Banning et al. discloses an instruction memory where memory pages marked with at T bit are protected and if a write is attempted, an exception is generated (Col. 1, line 60 – Col. 2, line 8). In this system, the T bit provides the protection so that the memory page is not writeable at the first privilege level. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Arora to provide the instruction memory protection disclosed by Banning et al. since doing so provides for valid, un-tampered memory instructions by protecting these instructions from being overwritten or changed.

The steps of the invention must occur at the call of an instruction since the operation of the system is governed by the instructions of instruction memory 36.

Regarding Claims 12, 17 and 23 Arora discloses a computer system comprising:

a processor (Figure 2, processor 30) having current privilege level which controls accessibility to the system resources (Column 1, lines 30-41 and Column 4, lines 13-27) and having a previous privilege level state (CPL 38),

a memory (Figure 2, Instruction memory 36) storing a privilege promotion instruction ("memory stores a plurality of instructions" such as an "EPC instruction which directs the processor to change the privilege level of the architectural current privilege level", see Column 3, lines 20-25 and Column 4, lines 13-27), and an operating system stored in the memory for controlling the processor and memory (operating system instructions are assigned one privilege level..., Col. 1, lines 30-41) and performing the privilege level promotion instruction as follows:

reading a stored previous privilege level state (register CPL 38 stores the privilege level

set by a previous instruction, Col. 4, lines 19-22),

comparing the read previous privilege level state (CPL 38) to the current privilege level

(comparing CPL to the instruction's privilege level, indicated by the EPC, wherein this case the

instruction's privilege level is the current privilege level and the stored privilege level is the

previous privilege level, column 6, lines 46-49. The privilege level stored in CPL 38 is the

previous privilege level since it represents a previous instruction, while the privilege level related

to the EPC is the current privilege level since it represents the current instruction);

and if the previous privilege level state is equal to or less privileged than the current

privilege level ("since the EPC instruction directs the processor to change the architectural

privilege level to a higher privilege level..." indicates that the CPL is less privileged than the

level indicated by the EPC), promoting the current privilege level to a second privilege level

which is higher than the first privilege level ("...increase the architectural privilege level from

privilege level 3 to privilege level 0" wherein privilege level 0 is more privileged). The

privilege level is promoted as the processor starts to operate at the higher privilege level

indicated by the EPC. In comparing privilege levels, the stored privilege level (stored in CPL 38)

must be read in the comparison process.

Arora does not teach the instruction memory 36 including a page of memory not

writeable by application instructions at a first privilege level.

Banning et al. discloses an instruction memory where memory pages marked with at T bit

are protected and if a write is attempted, an exception is generated (Col. 1, line 60 – Col. 2, line

8). In this system, the T bit provides the protection so that the memory page is not writeable at

the first privilege level. It would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the system of Arora to provide the instruction memory

protection disclosed by Banning et al. since doing so provides for valid, un-tampered memory

instructions by protecting these instructions from being overwritten or changed.

Regarding Claims 2, 8, 13, 19, and 24, Arora discloses the method of promoting a current

privilege level wherein the step of performing the privilege promotion instruction further

includes: if the previous privilege level state is more privileged then the current privilege level

("if the EPC instruction specifies a privilege level lower than or the same as the architectural

current privilege level..."), taking an illegal operation fault ("the processor will issue a fault",

Column 6, lines 55-61).

Regarding Claims 3, 9, 14, and 20, Arora discloses the method of promoting a current

privilege level wherein the system resources include system registers (architectural register set,

Column 3, lines 61-67).

Regarding Claims 4, 10, 15, and 21, Arora discloses the method of promoting a current

privilege level wherein the system resources include system instructions ("memory 36 stores a

plurality of instructions that are processed in the pipeline", column 3, lines 22-25).

Regarding Claims 5, 11, 16, and 22, Arora discloses the method of promoting a current

privilege level wherein the system resources include memory pages (Figure 2, instruction

memory 36).

Regarding Claim 7, and 18, Arora discloses the method of promoting a current privilege

level further comprising:

performing a return instruction including:

transferring instruction control flow to the stored return address to the first page of memory, and demoting the current privilege level to the stored previous privilege level ("a return instruction would instruct the processor to decrease the architectural current privilege level to the previous privilege level", Column 6, line 65-Column 7, line 3).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Midys Rojas whose telephone number is (571) 272-4207. The examiner can normally be reached on M-F 5:30am - 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sanjiv Shah can be reached on (571) 272-4098. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Midys Rojas/
Midys Rojas
Examiner
Art Unit 2185

MR

SANJIV SHAH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100